Portal-based Access to Advanced Security Infrastructures

J. Watt, R.O. Sinnott, T. Doherty, J. Jiang

National e-Science Centre, University of Glasgow, Glasgow G12 8QQ, UK
j.watt@nesc.gla.ac.uk

Keywords : Shibboleth, OMII-UK, PERMIS, GridSphere, PKI, PMI, SPAM-GP

Extended Abstract

Security and scalable user management is one of the key challenges facing the e-Research community. The very nature of deploying new Grid-enabled services involves the adoption of robust and highly complex underlying technologies such as PKIs. When used correctly, these tools allow many problems in the security domain to be tackled effectively, however in the hands of the inexperienced user, the complexities of building and using these technologies can expose the system to the same weaknesses that the system is trying to mitigate.

OMII-UK aims to provide a core toolkit for download which automates the installation and configuration of tools like the Globus Toolkit as much as possible. Under the auspices of the OMII SPAM-GP project, NeSC Glasgow has been investigating providing JSR-168 portlet-based access to several key technologies in the security realm. Most effort in the UK community has been focussed on interfacing these technologies with large-scale resources such as the NGS, but there is still a scarcity of simple tools to allow remote sites to run up their own well-protected grid services.

Shibboleth is fast becoming the de-facto solution to federated access management, allowing a user's home credential, which previously only had meaning at the user's institution, to be asserted reliably across a federation of trusted sites. SAML is used to transfer further information about a user to Service Providers, usually in the form of text string attributes. However it is normally the case that Services receive more information (from more Identity Provider sites) than they require. The SCAMP (Scoped Attribute Management Portlet) allows an administrator to edit the Service Provider's Attribute Acceptance Policy (AAP) to only allow specific regular expressions from chosen Identity Providers using a GUI rather than editing raw XML. This protects user confidentiality by only allowing the minimum amount of user information required to access protected services ever being exposed.

OMII supplies a GridSphere 2.2 portal infrastructure to deploy portlet services. By default, GridSphere has a fairly coarse-grained access control policy which controls which users see which portlets based on some generic user roles stored in a local database. Yet in a complete federated system, it would be Shibboleth that should be providing this role information. The Content Configuration Portlet (CCP) has solved this problem by developing both a dedicated Shibboleth Authentication plug-in for GridSphere, and a role-mapping portlet for allocating roles asserted by Shibboleth to individual portlets. This means any user logging in via Shibboleth would only see the specific portlets they are authorised to invoke, based on externally provided roles.

As a technology for providing a generic authorisation infrastructure for access to a variety of services, PERMIS is an ideal solution. The Attribute Certificate Portlet (ACP) allows an administrator (or delegated user) to issue X.509 Attribute Certificates (ACs) to local users, containing pre-agreed roles for access to local OR external services. An externally hosted PERMIS-protected service would, at the start of a collaboration, be configured to accept the local authority as a trusted signer and search the local attribute authority for ACs assigned to that user. Note that here, Virtual Organisations are being implemented in a de-centralised fashion, meaning that every service in the collaboration is free to configure its PERMIS policy any way it chooses. All the collaboration needs to do is agree the attribute rules that will be used across the sites for access, then individual sites control the issuance of Shibboleth and PERMIS credentials.

Using these tools all together, an administrator would be made aware of a new project, and the agreed text string attribute that Shibboleth can assert for user access. Using SCAMP, the service can be configured only to accept forms of this attribute string from the collaborating sites. The CCP can configure the user portal view based on these attributes, then the ACP can issue the required ACs containing the signed attribute string for its local users for any required services.

SPAM-GP will be tested in a real use-case scenario supporting the SEE-GEO project, securing portal based access to a geographical and census data linking service, with the backend services protected by PERMIS. This will allow the data centres to set their own access policies, but leave user management to the individual collaborating sites.

University of Glasgow | National e-Science Centre

Portal-based Access to Advanced Security Infrastructures

John Watt

UK e-Science All Hands Meeting

September 11th 2008

University of Glasgow | National e-Science Centre

Problem No. 1

- User management
  - Historically done by providers of services
    - Custom access control lists
      - Maps user to rights on system
      - Admin burden as user numbers skyrocket
    - User registration required
      - Face to face? Terms and conditions?
    - User revocation process is essential
      - User registered on many resources, always out-of-date info
  - Certification Authority
    - National-level identity – well recognised
      - Still requires devolved user registration process (RA)
  - Solution: Federated Access Management…

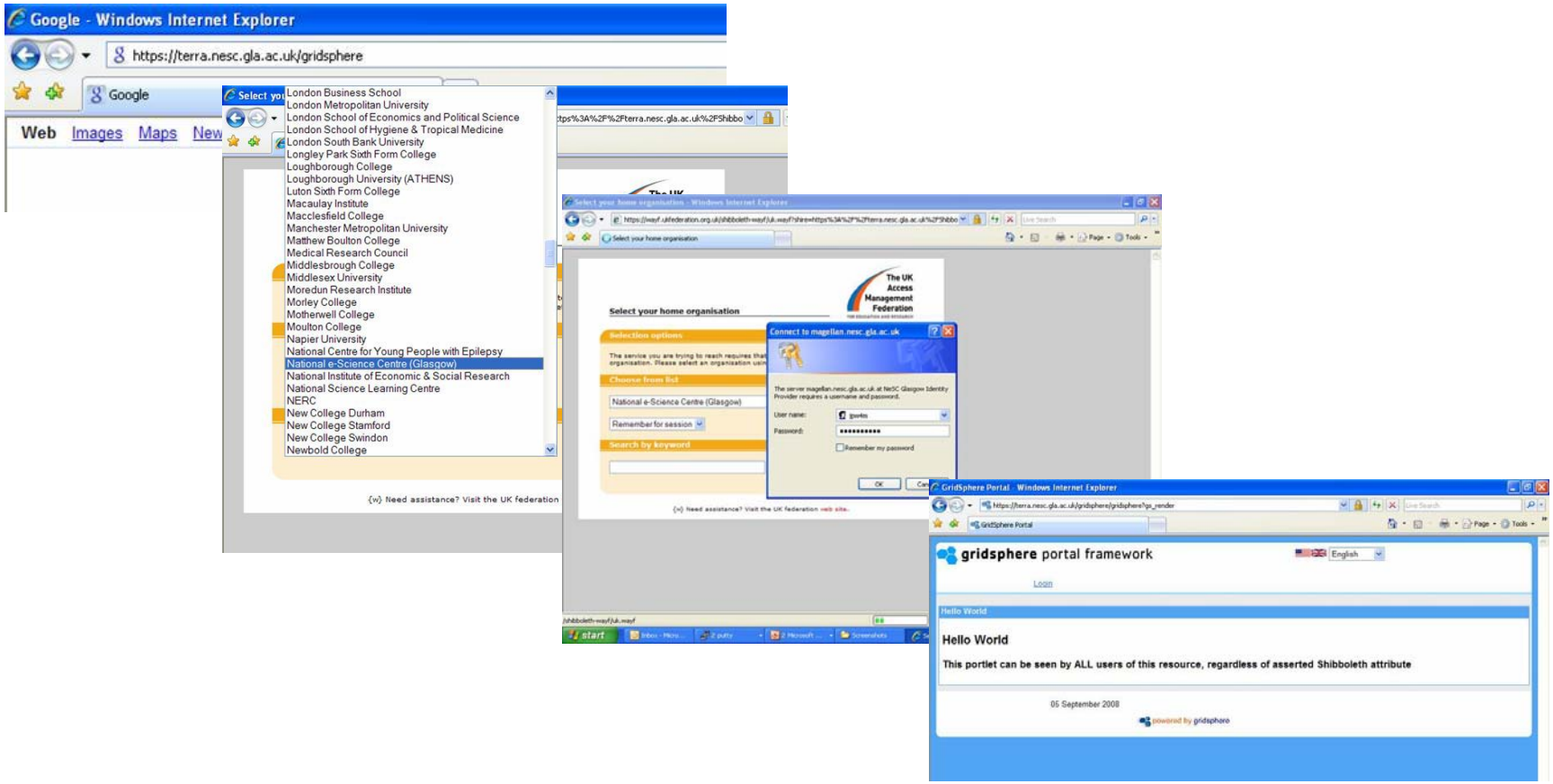
University of Glasgow | National e-Science Centre

Shibboleth (SAML)

- Implements a federation of trusting sites who agree to recognise the identity assertions of their federation partners
  - Federation manages registration and dissemination of current trusted sites
  - Defines Identity Providers (IdPs) and Service Providers (SPs)
    - IdP is an entity that has promised to correctly assert and verify the identity of its local users
      - Hence, user identity within fed. resources is reliable
      - ***Also supplies extra user info in SAML Attributes***
    - SP is a resource provider that accepts incoming federation authentication assertions as valid.

University of Glasgow | National e-Science Centre

Logging In to a Service



- Input service URL, choose IdP, enter credentials, service

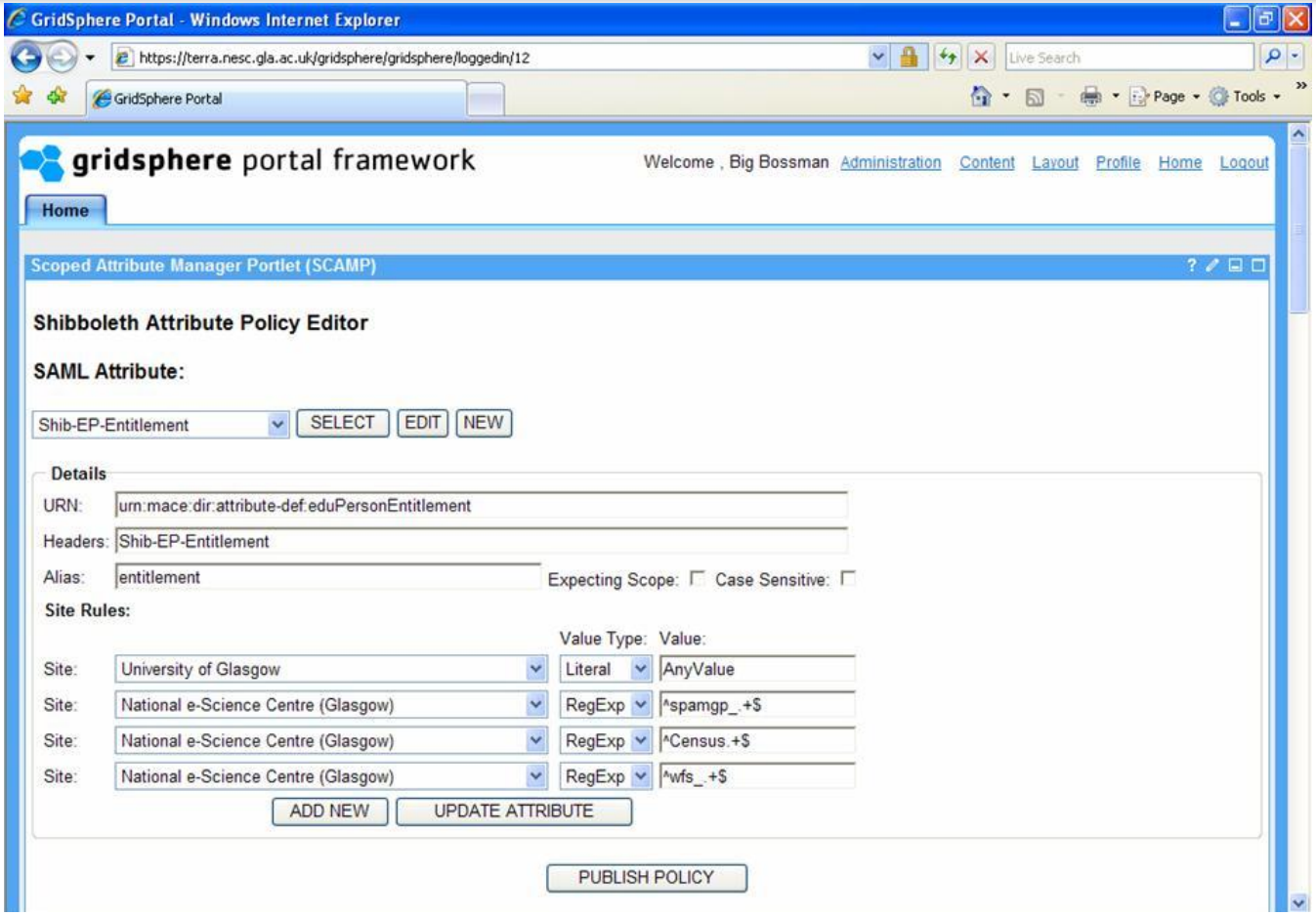
University of Glasgow | National e-Science Centre

Shibboleth (SAML)

- May not be desirable for an SP to accept EVERY IdP in the federation
  - The Shibboleth Attribute Acceptance Policy (AAP) defines the SP rules for accepting:
    - Identity Providers
    - SAML Attribute types
    - SAML Attribute values
  - The Scoped Attribute Management Portlet (SCAMP) allows this policy to be formally created
    - Produces consistent XML based on the administrator's policy requirements

University of Glasgow | National e-Science Centre

SCAMP



- Policy Editor tool
  - Defines valid IdPs, SAML attributes values and types

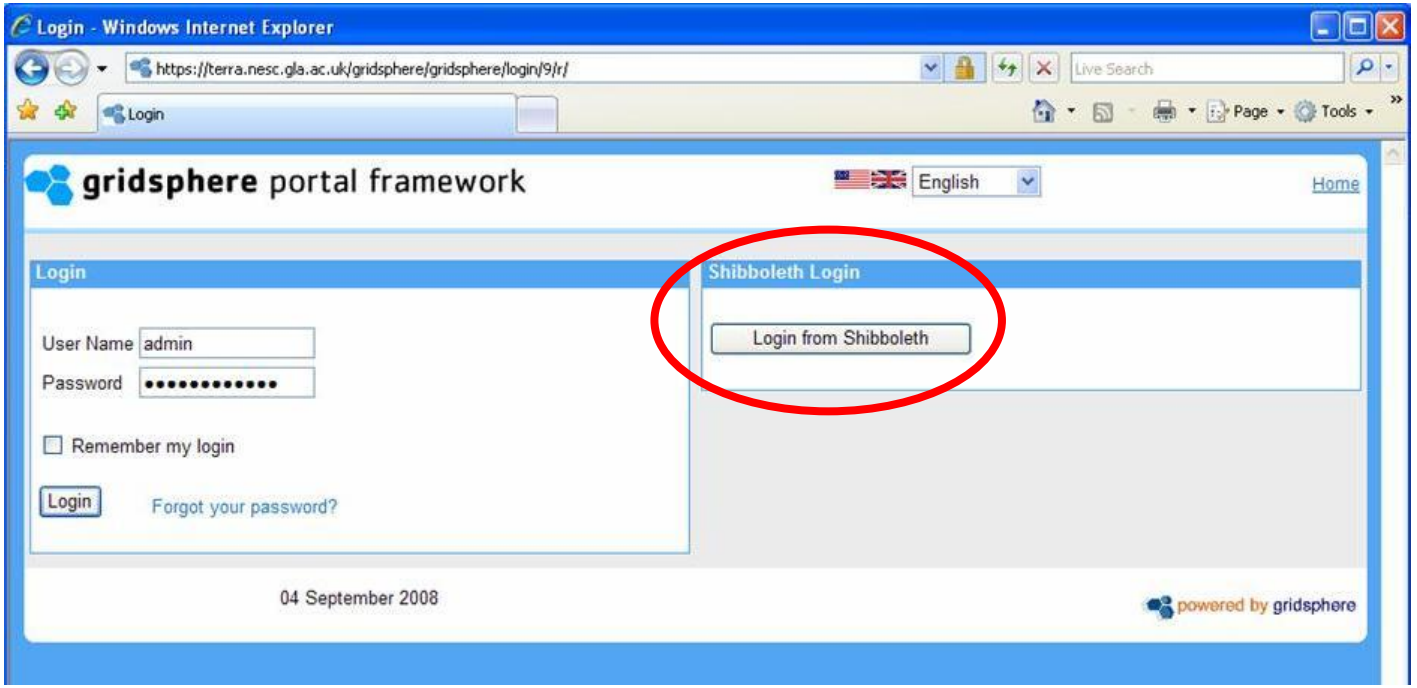
University of Glasgow | National e-Science Centre

Problem No. 2

- Single sign-on
  - Shibboleth enables one-time-password access for federation services.
  - But services need to be able to utilise Shibboleth provided information to enforce access control
  - Need to ALSO login to deployed portlet containers/apps to utilise their user management capability
    - For GridSphere, we need to define a new authentication module/framework
      - JAAS? – Couldn't get it to work
      - Custom module? – Failed for GS2.2.X
      - MAMS Shibbolized GridSphere – Yes
        - » Requires modification to handle complex Shibboleth roles

University of Glasgow | National e-Science Centre

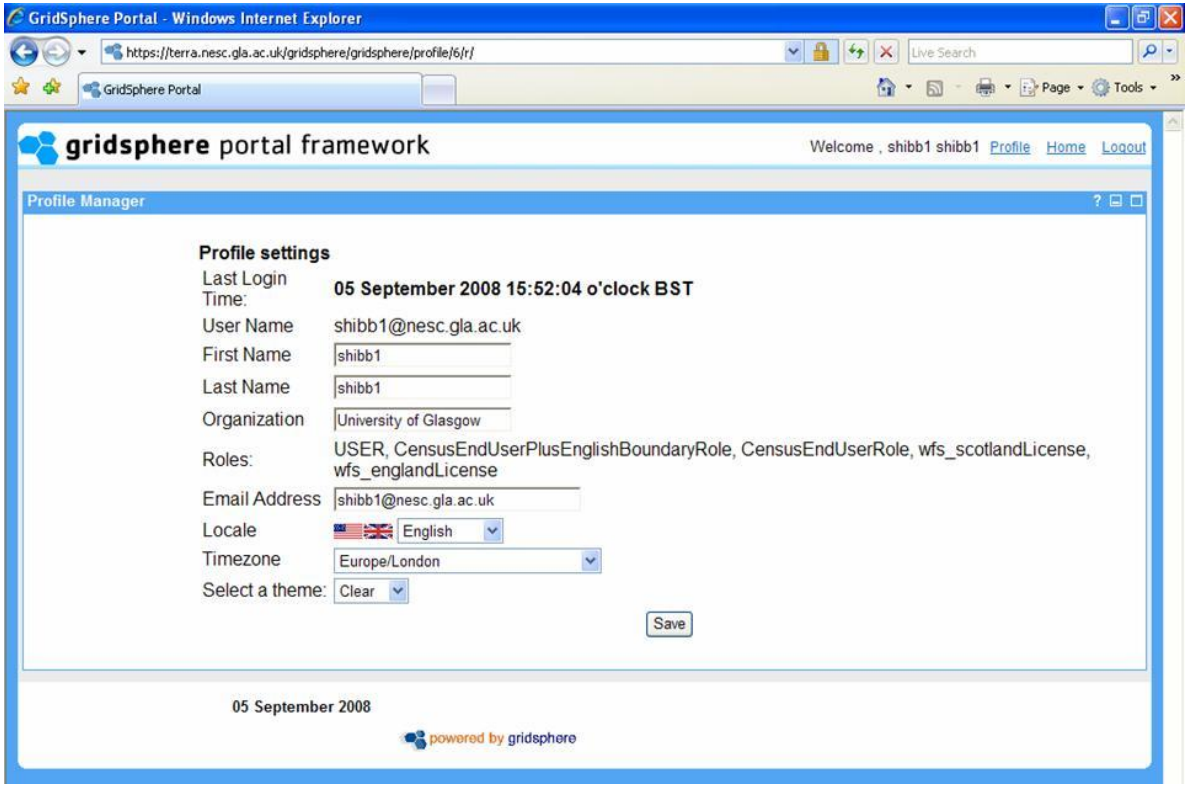
Content Configuration



- Module provides alternate login to GridSphere
  - Picks up active Shibboleth credentials and builds GridSphere login session from this information

University of Glasgow | National e-Science Centre

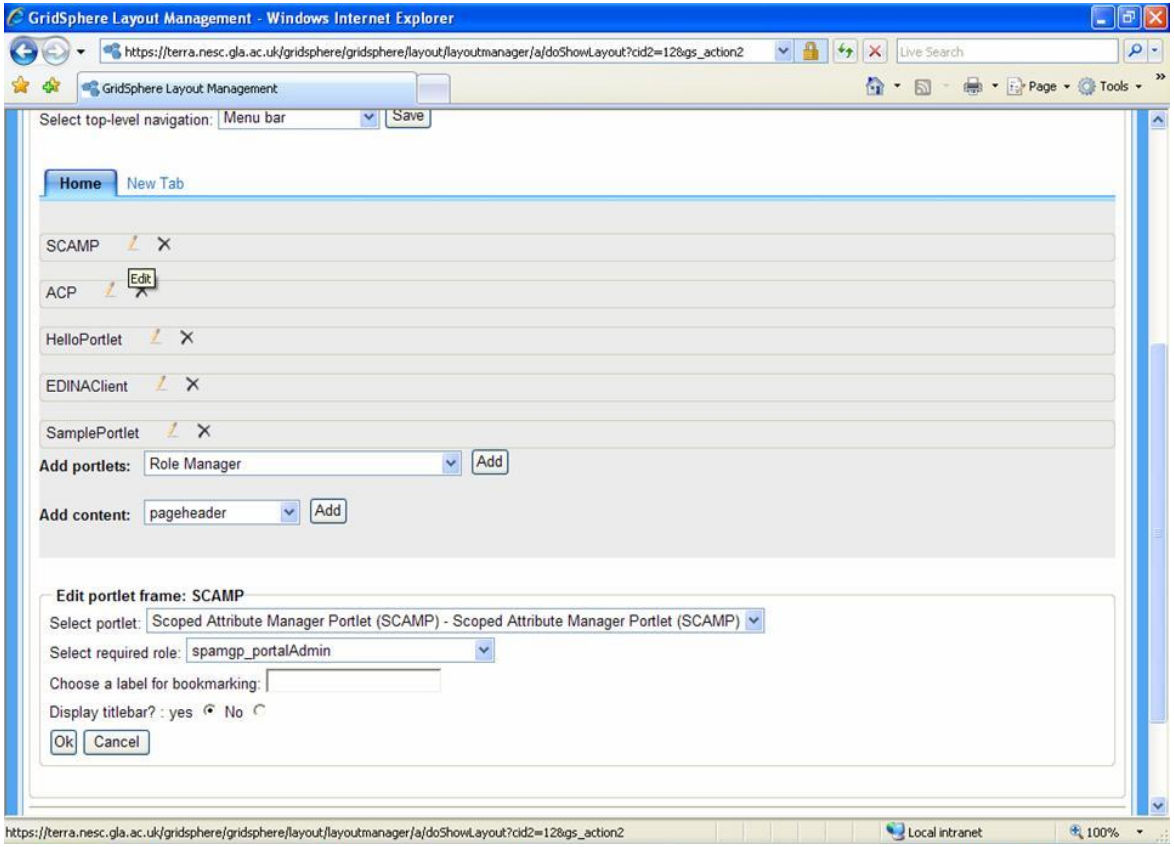
Content Configuration



- GridSphere now has an established user session with externally provided (from SAML) access privileges
  - In addition to the custom GridSphere roles (USER, ADMIN, SUPER)

University of Glasgow | National e-Science Centre

Content Configuration



- Layout manager can be used to assign Role Based Access Control on individual portlets

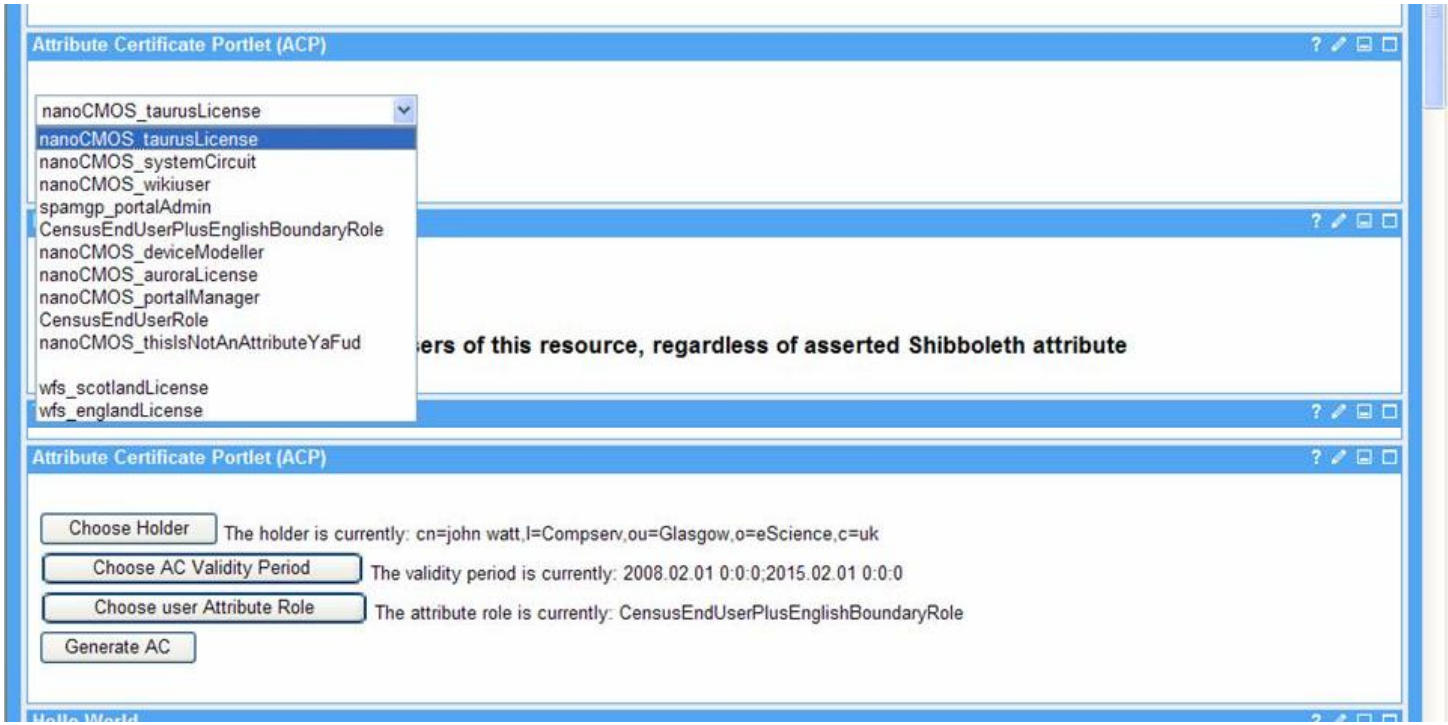
University of Glasgow | National e-Science Centre

Problem No. 3

- Have presented solution for portal based access control
  - Doesn't allow access to external security infrastructures
  - Scenario: protected service has a policy requiring a signed assertion of a user's role, traceable to a reliable Source of Authority, with a finite validity
    - PERMIS
  - Need to issue local users with X.509 Attribute Certificates for access to these services…

University of Glasgow | National e-Science Centre

Attribute Certificate Portlet



- Portlet allows a privileged user to issue Attribute Certificates (based on Shibboleth-provided roles if required) to users and store in LDAP
  - ‘privileged user’ may be local admin who has been delegated ability to assign attributes, OR, the admin of the external service who has been given attribute assignment privileges within the portal

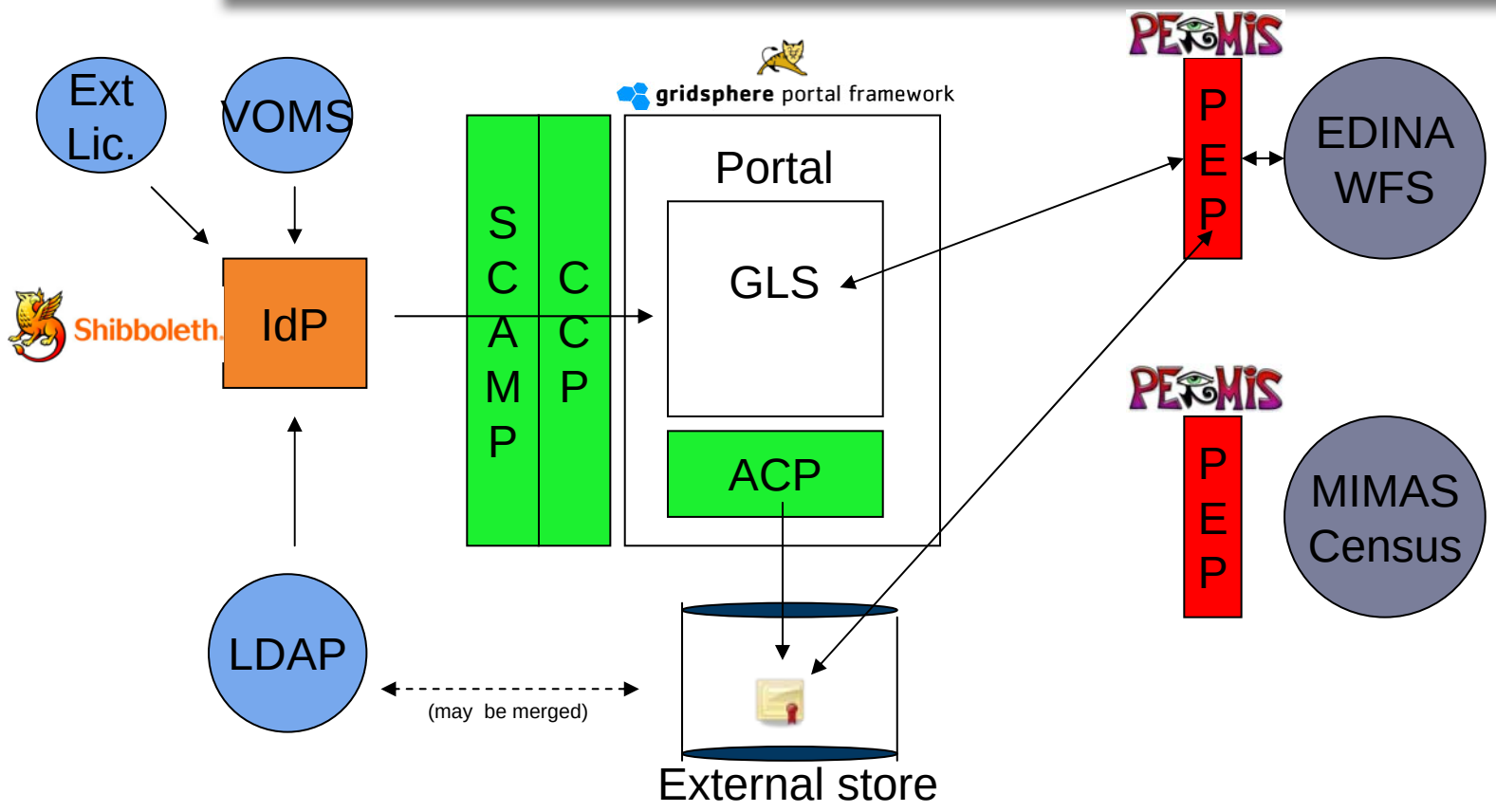
University of Glasgow | National e-Science Centre

SPAM-GP Deployment

- Presence in SEE-GEO and DAMES
  - PERMIS-protected GT4 services accessed through an RBAC-enabled portal utilising SAML-provided information
- ACP and SCAMP
  - Unzip .tar.gz file and ‘ant deploy’
- CCP
  - Requires change to GridSphere source and re-installation

University of Glasgow | National e-Science Centre

Security for SEE-GEO GLS Client



- SPAM-GP tools in green

University of Glasgow | National e-Science Centre

Status

- SCAMP code complete
  - May require slight alteration for “100%” JSR-168
  - Submitted for evaluation, docs available
- ACP functional
  - Requires user interface clean-up
  - PERMIS license issues
- CCP
  - Have a deployable solution that draws on MAMS software
  - Alterations documented
- ARP & PERMIS policy editor (not done)
  - Relegated as they are essentially SP-external
  - Tools have emerged that provide this functionality (ARPeditor, ShARPe…)

- All tools will be utilised in future NeSC projects, so improvements/augmentations are inevitable